Taking care of client data: what notaries need to know about computer systems, cybercrime and how to stay safe online

CONTENTS

1. Introduction

Earlier in the year this program was accredited by the Faculty Office for Continuing Professional Education (CPE) under the title "taking care of client data". Since then, the topic of data protection and cyber security has made headline news. On Sunday 28th May 2017, the Guardian newspaper published a "Business Reporter" cyber security special. Articles included "why it pays to heed the human factor in your cyber defence", "after the NHS hacking scandal could be Internet of things be next" and "people get ready: GDPR is coming!

And you may have seen billboards at some railway stations published by Hiscox: SMALL BUSINESS IS BIG BUSINESS TO CYBERCRIMINALS: it certainly is; cybercrime is a numbers game. It's not usually personal - but ... what if information about a client that could only have come from you, hit the headlines! What if the sensitive client data held by you is directly targeted?

After the malware infection that badly affected the NHS (costing $72,000 in ransom fees worldwide) and the problems experienced by BA - supposedly a power failure, how may notaries protect themselves?

Forty percent of notaries bill less than £10,000 in fees each year, nevertheless they are obliged to take data protection very seriously, indeed, a whole chapter in the Code of Practice is dedicated to the topic of data protection.

The Code states: -

- **"You implement appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."**

Surely this must now include the effect of cybercrime where "loss" is not accidental.

In this program, we consider the appropriate and proportional steps that may be taken to comply as we consider 'what kind of notary are you?'. Do you work from home, possibly part time, or maybe you combine notarial work with a busy caseload within a solicitors practice, perhaps you have extended responsibilities in that you oversee data security for the whole firm? In Section One, chapter 2, I write about appropriate and proportional computer hardware and software configurations for each 'kind of notary'.

Section 4 is about cybercrime; the nature of cybercrime and how it could affect the safety of your precious client data, seriously upset your peace of mind, damage both your financial health and the effect it could have on the reputation of the notarial professional. In Chapter 5 I discuss ways of how you may go about protecting your computer system against cybercrime. Chapter 6 provides an overview check list on how to 'stay safe online'

As most notaries are aware, their profession flies under the radar; even many solicitors are not sure what work is undertaken by notaries public: given the very sensitive nature of much of the client data which is recorded by notaries, this is probably a good thing. Most cybercrime is about money, however more dangerous to the profession would be a targeted attack, often known as spear phishing. This could be

where client data would be used and acted upon for a blackmail attempt directed to the data subject, industrial espionage or some other nefarious reason.

> It's tempting to view security breaches as the products of mastermind hackers, but the sad reality is most of the time, breaches are the result of people falling for plain old trick emails

Chapter 6 includes a 'forensic' examination of fake emails.

Section three is all about the data; as a notary, you could just make a written note of the six things you need to record and keep this information locked safely away, protected against fire or theft. Much more likely you will photocopy a passport, utility bill and either the whole or part of document you are notarising, this may be attached to a completed-by-the-client a registration type form.

With the cost of easy-to-use technology at an all-time low, you probably scan and save the documents on a computer system. Now you have data in digital format and the fun begins

- Managing multiple copies

The client may request a scan to be emailed to them; this is easily done however an extra copy is created that now sits in your 'sent items' box. Of course, you know that computer systems must be backed up;

a sensible procedure is the' Grandfather, father, son' system where three copies are made. In case one backup fails you go back a version. Going forward, the 'grandfather' version is overridden. Oh, but what about a 'snapshot' of client data as it was three months ago!

Chapter 9 focuses on where and how data is stored and disaster recovery strategies.

Chapter 10 discusses the data protection legislation. "Organisations that collect and manage your personal information must also protect it from misuse and respect certain rights".

Everyone has the right to the protection of personal data.

Some people find information technology (IT) endlessly fascinating, for others IT is terrifying. Technophile or technophobic – this booklet is for you as I describe the minimum, in simple terms, about what that you as a notary NEED to know about being safe online. And for the technophiles, there's a lot more besides.

Please note: these notes are based on computer systems using Microsoft's Windows Operating Systems. As there are many versions and, as this is not a how-to-use-a-computer tutorial, some of the detailed instructions may not apply to your system.

Any questions or feedback; please contact Lisa Preuveneers lisa@lawconsultancyservices.co.uk